IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

Security Enhancement for Federated Fog Computing and Enhanced IoT in Network Function Virtualization

Prof. A M Prasad, Yashaswini G

Dept of CSE, Dayananda Sagar College of Engineering, Bangalore, India

M.Tech Student, Dept of CSE, Dayananda Sagar College of Engineering, Bangalore, India

ABSTRACT*:* Smart IoT applications require connecting multiple IoT devices and networks with multiple services running in fog and cloud computing platforms. One approach to connecting IoT devices with cloud and fog services is to create a federated virtual network. The main benefit of this approach is that IoT devices can then interact with multiple remote services using an application specific federated network where no traffic from other applications passes. In this projecr we propose to extend a federated cloud networking security architecture so that it can secure IoT devices and networks and it can also performas the load balancing of the dataSmart IoT applications require connecting multiple IoT devices and networks with multiple services running in fog and cloud computing platforms. In this projecr we propose to extend a federated cloud networking security architecture so that it can secure IoT devices and networks and it can also performas the load balancing of the data

I.INTRODUCTION

The security architecture is based on the concepts of NFV and SFC for composing security services. In this paper we describe how to integrate a federation agent in an IoT gateway or network controller (Can bus, 6LowPan, Lora, ...). We discuss how we could integrate a lightweight NFV/SFC functionality with the IoT gateway. We also discuss recent research on using virtual networks over the IoT network and its usefulness. In particular, if virtual networks are available over IoT networks, then they can also be federated and thus isolated. We also .discuss issues related to federating virtual networks that use different protocols.

The presented architecture contains 3 components mainly:1) Federated netwmanager 2) Network agent 3) Datapath proxy. The Federated Network Manager is the software component that provides a uniform interface for users in order to set up a virtual federated network in a transparent way, independently from the underlying clouds. In order to do this, it features an API to allow for federated network definitions, and uses adaptors to talk to the Cloud Management Platforms. The Network Agent drives the control plane of a federated network. It informs other Network Agents about the known networks in its domain, and instructs the Datapath proxy. The Network Agent is present with a well-known endpoint in the cloud infrastructure. The Network Agent provides a REST API to communicate with the Federated Network Manager and other peer Network Agents.

II.BACKGROUND WORK

Encryption searches enable keyword searches with encrypted information. The concept of public key encryption with keyword search (PEKS) has been proposed by Boneh et al [12], which is important for protecting the privacy of exported data. The owners of data in the PEKS schemes [7], [8], [16] keep their forms in a format hidden from a remote data server that is not trusted. Data users want to query on the hidden ry les by generating a keydo trapdoor, and the data server performs a search operation. The water et al. [5] showed that the PEKS scheme can be used to build searchable logs. Later, Xu et al. [17] presented a general framework for combining PEKS with keyword search without concrete. Tang [18]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

proposed a multidimensional encryption scheme that can be performed along with a pairing scheme. In 2016, Chen et al. [3] introduced the "dual-server" concept in PEKS to resist guessing of a foreign keyword attack. Yang et al. [19] introduced a provisional and time-limited encryption mechanism for a representative on the PEKS system to monitor the deployment of time-controlled authorities. Wang et al. [1] proposed a coded keyword search program for unmatched accessibility, in which order-save symmetric en-cryption was used [35]. Cao et al. [3] designed a novel system to recognize searches for multiple keywords. Readability writing is also studied in [20], [21], [22]. In the context of Attribute-based Encryption (ABE), Sa-hai and Waters [41] originally introduced the concept of ABE, which was subsequently published by Goyal et al. [15]. In particular, Goyal et al. comes with Key-Policy Attribute-based Encryption (KP-ABE) and Cipher textPolicy Attribute-based Encryption (CP-ABE). Since then, a list of ABE strategies has been proposed in the literature [9], [18], [19]. While these programs are designed to achieve improvement, transparency and security, they do not address tracking and dismissal issues. Li et al. introduces a responsive CP-ABE view [23] to prevent unauthorized key distribution among embedded users. In a recent work [22], a multi-user CP-ABE response plan was proposed. Liu et al. we have also proposed a white box [17] and a black-box [16] protocol for 1 CP-ABE systems that support policy clarity on any monotone access structures. buildings. Ning et al. [20], propose several effective CP-ABE systems with white box tracking and black box tracking. Deng et al. [11] pro-vide CP-ABE approach to obtain mature access credentials in the cloud storage system.

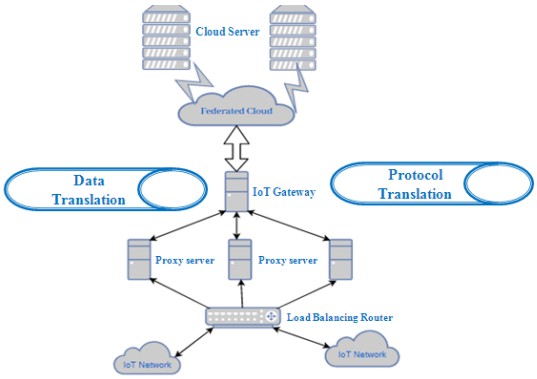

Figure 1: Proposed architecture model

A number of multidisciplinary solutions to CP-ABE systems have also been proposed in the literature, such as. Sahai et al. [22] corrects the problem of duplicate maintenance and provides a completely secure construction of ABE based on the distributed power supply. Yang et al. [24] propose a CP-ABE system for an inaccessible and accessible security back and forth. Recently, Yang et al. [5] propose a method for updating the attribute to achieve a dynamic change in the attribute (such as updating the previous attribute and re-assigning the previously specified attribute). However, the aforementioned studies do not address the mistreatment of key reproductive authorities, the possibility of investigation, and the exclusion (of misconduct). these are the problems we are looking to fix in this paper.

III.PROPOSED APPROACH

we have proposed an architecture for securely connecting IoT devices with remote federated cloud services. The communication between IoT network with federated fog network through proxy federation agents or proxy IoT gateways. We will place load balancing router between the IoT network and proxy IoT gateways. The loadbalancing router attempts to route Internet traffic optimally across different gateways. If any gateways is down then its computation work will be router to other gateway in the pool. The proposed IoT gateway is responsible for the protocol translation between the IoT network with federated fog cloud.

Figure 1 shows the proposed model of an architecture for securely connecting IoT devices with remote federated cloud services. First the data transmission starts from the IoT network And then it is sent to the load balancing router where it performs the task of balancing and sharing the load in a network with help of multiple internet connectivity options and network link resources. From the load balancing router the data is transmitted to the proxy servers, where all the three

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

proxy servers shares required data, and then it sends to IoT gateway. We can also see there are Data translation and Protocol translation where the protocol is translated from one form to another form(e.g, the protocol is translated from HTTP to RTCP). Here there is no down of gateway so that the data can be easily transmitted easily. If there is a down in IoT gateway we can easily transmit data from proxy server to federated cloud directly.

MECHANISM OF DATA TRANSMISSION W

hen two different IoT networks connect to the cloud, it is IoT Gateways responsibility to convert the control data into the cloud protocols (e.g. HTTP).This data/control data translation is not addressed in the Existing system. The data transmitted from IoT network is the real time data which requires QoS, Which is not addressed in the existing system. In order to transport the data from IoT network controller to the cloud, there is a need to translate the IoT data into a protocol understandable by the Cloud network. First, this translation is done by the IoT Gateway, then the data is sent by the IoT Gateway into a cloud, which provides advanced network services, such as FW and DPI, collects the data and performs higher-level processing and analysis.

IV.PERFORMANCE EVALUATION AND EXPERIMENTAL RESULTS

In this section, we evaluate the performance of the proposed systems presented in sections 7 and 8. The tests were performed on a laptop containing the following information: Intel Core i5-5200U, 2.20 GHz, 4 GB memory, and Windows 7 operating system via Service Pack 1. We use a cryptography based pairing library [28] in A1 curve to detect proposed plans. The programming language used is Java with JDK32-1.6.0 and JPBC-2.0.0 [10].

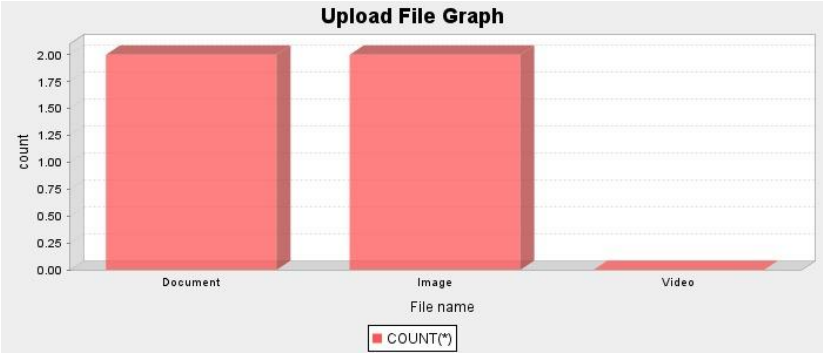

Figure 2. Load balancing graph for different type of data

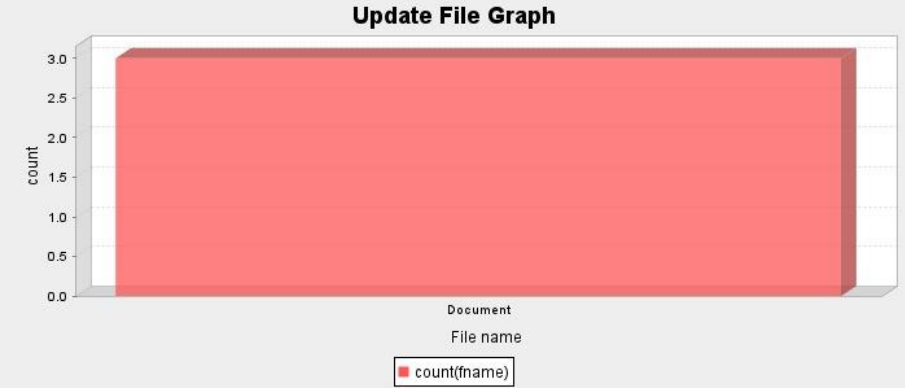

Figure 2. File update graph for different type of data

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

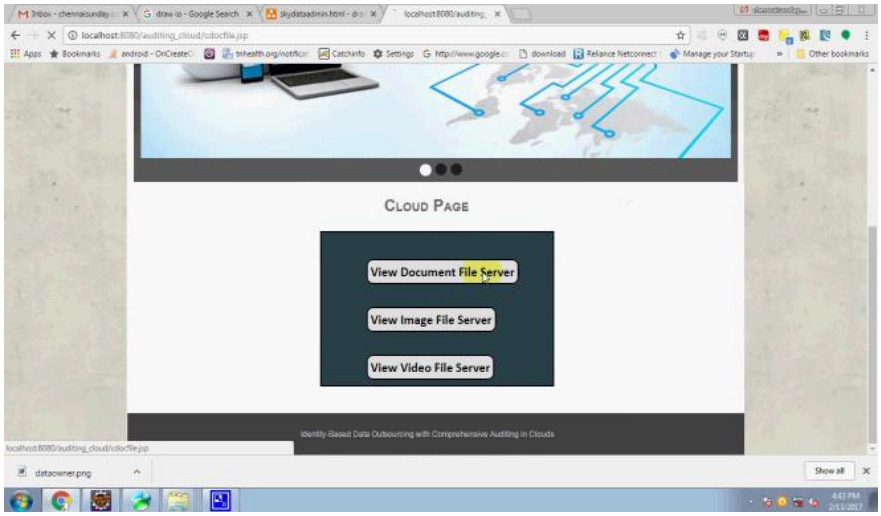

Figure 3: Cloud storage page.

Figure 4: File owner details

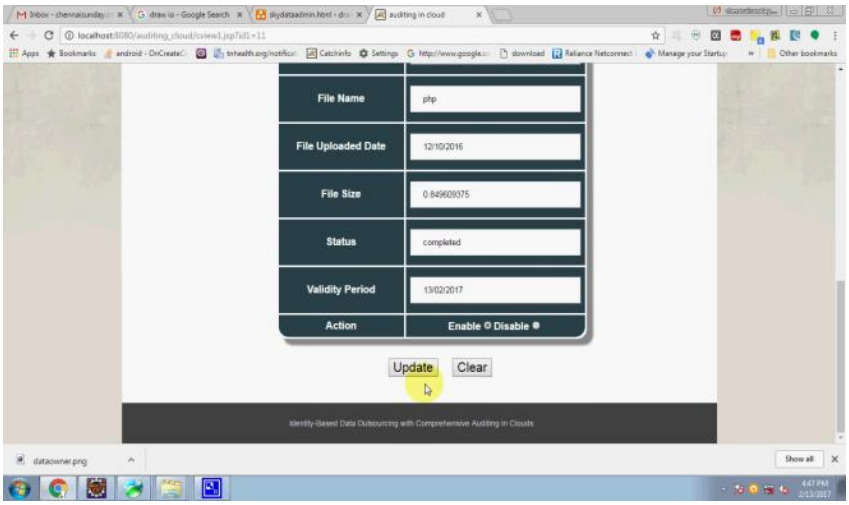

Figure 5: Access permissions update

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

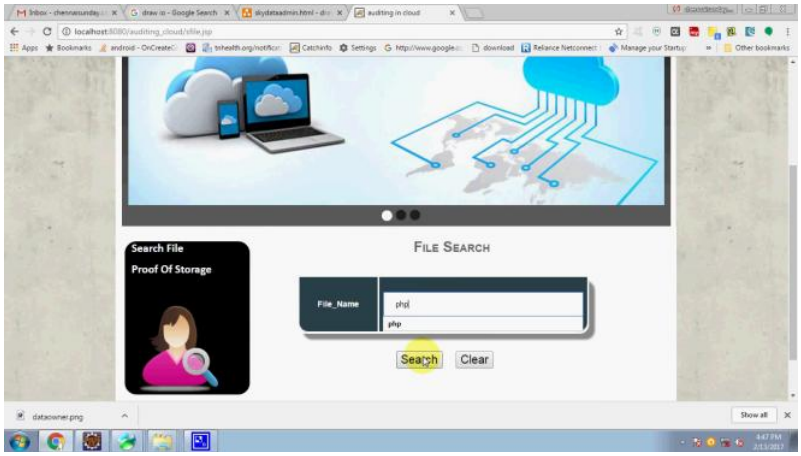

Figure 6: File search at the cloud

Figure 7: Auditor page

V.DISCUSSION AND FUTURE WORK

Network Virtualization in IoT Networks and Federation of Virtual IoT Networks

Starting from the assumptions conducted in [22], where authors figured out the necessity to extend the Network Virtualization capabilities from stable infrastructure towards dynamic IoT Virtual Networks, we consider our current work as the beginning step in this direction. Our idea is to extend the networking federation concept pushed on the Edge (that is NFV/SFC in the Edge) where many IoT and Gateways are taken into account. All future scenarios will be created from complex configurations of interconnected devices where security and privacy need to be heavily addressed. Researchers need to consider different administrative domains where devices belong to, hence dealing with federation capabilities in security, leveraging different technologies (heterogeneity). In this latter, we look at these new compelling functionalities, introducing abstractions and slicing ([12]) of resources

VI.CONCLUSION

The emphasis on access control and keyword search support are key issues in secure cloud storage. In this work, we outlined a new paradigm for inaccessible encryption, and proposed a concrete architecture that allows us to track and retrieve dangerous cloud users (leaky warranties). Our method can also be used in cases where user credentials are distributed by trusted administrators. We note that we may need black box tracking, which is a strong idea (compared to white box tracking), in the current way. One of our future tasks is to process black box tracking and auditing. In addition,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906189 |

the AU is thought to be completely reliable in the current way. However, in practice, it may not be the case. Is there a way to reduce trust from the AU? Ideally, one way is to use multiple AUs. This is similar to the strategy used in divination programs. But it will require more communication and distribution costs and in the meantime, the problem of integration between AUs continues. An alternative approach is to use secure hiring of multiple parties in the presence of adversarial opponents. However, it works well and is a bottle. Establishing a multi-party coalition and relying on AU divisions (while maintaining the same level of security and efficiency) is also part of our future work.

REFERENCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404,2017.
[2] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.
[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patter-son, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.
[4] Nuttapong Attrapadung and Hideki Imai. Attribute-based en-cryption supporting direct/indirect revocation modes. In Cryptog-raphy and Coding, pages 278–300. Springer, 2009.
[5] Amos Beimel. Secure schemes for secret sharing and key distribution.PhD thesis, PhD thesis, Israel Institute of Technology, Technion,Haifa, Israel, 1996.
[6] Mihir Bellare and Oded Goldreich. On defining proofs of knowl-edge. In Advances in Cryptology-CRYPTO'92, pages 390–420.Springer, 1993.
[7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
[8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasi-lakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal,4(1):75–87, 2017.
[9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual systemABE in prime-order groups via predicate encodings. In Advancesin Cryptology - EUROCRYPT 2015, pages 595–624, 2015.
[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing basedcryptography. In ISCC 2011, pages 850–855. IEEE, 2011.
[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang,and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.
[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasi-lakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.
[13] Vipul Goyal. Reducing trust in the PKG in identity based cryp-tosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447.Springer, 2007.
[14] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.
[15] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of en-crypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details